Authors:

CHANDNI AGRAWAL, ABDULLAH ZINJANI, PRIYAVARDINI CHANDRASEKARAN, DEEPTI MURMU, PAWAN PRAKASH, KALAIPRIYA J
Tata Consultancy Services, India.

Abstract:

The authentication and authorization have been constant areas of concern to reduce password fatigue and security threats. Mainframe systems have been the most relied solution so far for bulk data management and processing. But when user friendliness needs to be incorporated with security, single sign on proves to be an effective quick fix for mainframe applications. In mainframes, we can implement SSO by using EIBTRMID and EIBTIME variables. These variables enable us to get the system terminal ID and time. When the session time expires, a login page opens if we request to traverse through a particular application. The login page is opened even when our terminal ID changes. We store the terminal ID in the table. Whenever the system generates a terminal ID, it is moved to host variable and updated in the table. In a new session , when the user requests for the application , the login page opens since the terminal ID is new and it does not match with the one in the table. When the same user tries to request for some other application within the same session and before the session expires, logging-in is not required as the terminal ID is the same. To add on to security of single sign on, we have amalgamated it with Single Sign Out which reinforces the authoritative aspects for an authenticated user. Embracing the application with Single Sign Out completes the circle assuring that the user is automatically signed out from the related applications once he logs out from any one of the applications.